

Usługa mLegitymacja szkolna w Aplikacji mObywatel – dostępne funkcje, ochrona danych osobowych

Usługa pozwala korzystać z mLegitymacji szkolnej – dokumentu elektronicznego, który ma taką samą funkcję i moc prawną, jak legitymacja wydana w wersji papierowej lub w postaci plastikowej karty (e-legitymacji).

Za pomocą Usługi mLegitymacja szkolna możesz:

- potwierdzić, że jesteś uczniem danej szkoły,
- skorzystać z ulg i zwolnień, które przysługują po okazaniu legitymacji.

Ilekcioć w załączniku pojawia się pojęcie pisane wielką literą i niezdefiniowane w definicjach to ma ono znaczenie nadane im przez Regulamin.

§ 1. Definicje:

1. **Certyfikat Ucznia** – poświadczenie, o którym mowa w art. 19e w ust. 2b pkt 1 ustawy o informatyzacji, pozwalające na potwierdzenie integralności i pochodzenia dokumentów elektronicznych oraz potwierdzenie lub przekazanie danych osobowych Użytkownika wydany w ramach usługi mLegitymacja szkolna.
2. **System** – system teleinformatyczny zapewniany przez Ministra Cyfryzacji, który pozwala na wydanie przez Dyrektora szkoły mLegitymacji szkolnej i wygenerowanie danych osobowych ucznia oraz danych potwierdzających status mLegitymacji szkolnej.
3. **Dyrektor** – Dyrektor szkoły, do której uczęszcza Uczeń lub upoważniona przez Dyrektora osoba wydająca mLegitymację szkolną.

§ 2. Informacje ogólne

1. Usługa stanowi „mLegitymację” w rozumieniu § 3 ust. 2 i nast. rozporządzenia Ministra Edukacji Narodowej w sprawie świadectw, dyplomów państwowych i innych druków (Dz.U. z 2019 r. poz. 1700, z późn. zm.) i jest dokumentem elektronicznym zawierającym dane dotyczące sytuacji prawnej użytkownika publicznej aplikacji mobilnej lub praw mu przysługujących, o którym mowa art. 19e ust. 2 pkt 2 ustawy o informatyzacji.
2. Dyrektor jest organem odpowiedzialnym za wydanie (aktywowanie) oraz ewentualne unieważnienie mLegitymacji szkolnej.

§ 3. Użytkownicy

1. Użytkownikami Usługi mLegitymacja szkolna zwanej dalej „mLegitymacją”, mogą być wyłącznie osoby, które spełniają dwa poniższe warunki:
 - 1) posiadają nadany numer PESEL;
 - 2) są uczniami szkoły podstawowej, ponadpodstawowej, szkoły policealnej lub słuchaczami szkoły dla dorosłych, którym właściwi Dyrektorzy wydali mLegitymację.– zwani dalej w niniejszym załączniku „**Uczniami**” lub pojedynczo „**Uczniem**”.

2. Zabrania się Uczniowi:
 - 1) udostępniania Aplikacji w celu posłużenia się nią przez inną osobę,
 - 2) udostępniania jednorazowego kodu QR oraz hasła otrzymanego od Dyrektora, umożliwiającego dostęp do Usługi.

§ 4. Aktywacja Usługi

1. Przy pierwszym użyciu Usługi dokonywana jest jej aktywacja.
2. Do przeprowadzenia aktywacji Usługi niezbędne jest aktywne połączenie internetowe.
3. Aktywacja Usługi polega na:
 - 1) wystąpieniu przez Ucznia (rodzica lub opiekuna prawnego w przypadku osób niepełnoletnich) do właściwego Dyrektora szkoły o wydanie mLegitymacji;
 - 2) nadaniu przez właściwego Dyrektora szkoły uprawnień w Systemie, wgraniu zdjęcia Ucznia w Systemie, wygenerowaniu kodu QR i jednorazowego kodu aktywującego mLegitymację;
 - 3) zalogowaniu do Aplikacji;
 - 4) wczytaniu kodu QR oraz wpisaniu przez Ucznia (rodzica lub opiekuna prawnego) kodu aktywacyjnego mLegitymacji;
 - 5) pobraniu danych osobowych Ucznia z Systemu.
4. Jednorazowy kod aktywacyjny oraz kod QR jest ważny 30 dni od momentu jego wygenerowania w Systemie.
5. Uczeń (rodzic lub opiekun prawny) może aktywować Usługę i pobrać dane Systemu wyłącznie na jednym urządzeniu mobilnym.
6. Po pobraniu danych z Systemu automatycznie jest tworzony i pobierany do Usługi Certyfikat Ucznia. Certyfikat przypisany jest do Ucznia i jego urządzenia mobilnego. W celu utworzenia Certyfikatu i zarządzania Certyfikatami Minister przetwarza dane osobowe Ucznia: imię, nazwisko i numer PESEL.
7. Certyfikat Ucznia służy również do pobrania i podpisania danych w usłudze mKDR, dla Uczniów posiadających Kartę Dużej Rodziny.
8. Ważność Certyfikatu jest ograniczona w czasie i jest tożsama z okresem ważności wydanej Uczniowi odpowiednio legitymacji szkolnej albo e-legitymacji szkolnej.
9. Nie jest możliwe nadanie uprawnień przez Dyrektora w Systemie oraz aktywacja Usługi – jeżeli Uczeń nie spełnia warunków określonych w § 3 ust. 1 niniejszego załącznika, w szczególności kiedy zostało zgłoszone zaginięcie lub uszkodzenie odpowiednio legitymacji lub e-legitymacji, bądź też w przypadku podjęcia próby aktywacji Usługi na kolejnym urządzeniu mobilnych.
10. Poza funkcjami elektronicznego przekazania danych oraz elektronicznej weryfikacji danych osobowych Aplikacja nie oferuje funkcji eksportu ani importu danych.

§ 5. Funkcje mLegitymacji

1. **Okazanie mLegitymacji na ekranie urządzenia mobilnego:**
 - 1) zgodne z przepisami prawa okazanie mLegitymacji ma skutek analogiczny jak okazanie legitymacji w postaci papierowej lub e-legitymacji;

- 2) pozwala ocenić osobie uprawnionej do kontroli legitymacji prawdziwość mLegitymacji szkolnej między innymi na podstawie następujących elementów graficznych:
 - a) zdjęcia osoby legitymowanej,
 - b) numeru legitymacji i wieku Ucznia,
 - c) statusu: „ważna” lub „nieważna”,
 - d) hologramu – którego wygląd pozwala na stwierdzenie, iż nie stanowi on statycznego obrazu, lecz jest faktycznie generowany przez Aplikację,
 - e) flagi Polski – której wygląd pozwala na stwierdzenie, iż nie stanowi ona statycznego obrazu, lecz jest faktycznie generowana przez Aplikację,
 - f) czasu okazania.

2. Przekazanie danych z usługi mLegitymacji do Aplikacji mWeryfikator

- 1) Elektroniczne przekazanie danych Ucznia użytkownikowi Aplikacji mWeryfikator umożliwia przesłanie niektórych danych w mLegitymacji do użytkownika Aplikacji mWeryfikator.
- 2) W tym celu Uczeń, który przekazuje dane, powinien:
 - a) wybrać funkcję „Przełącz” w Aplikacji;
 - b) po pojawieniu się odpowiedniego komunikatu wybrać i zaakceptować opcję „przekazanie danych”; Po wyświetleniu w Aplikacji kwadratowego kodu graficznego (dalej „Kod QR”) Użytkownik Aplikacji mWeryfikator może odczytać ten Kod QR za pomocą aparatu fotograficznego jego urządzenia mobilnego. Kod QR zawiera informację o czasie i jest ważny 10 minut od chwili jego wygenerowania. Po upływie tego czasu przekazanie danych wymaga ponownego wygenerowania Kodu QR;
 - c) Po prawidłowym zeskanowaniu Kodu QR pomiędzy urządzeniami mobilnymi Ucznia i użytkownika aplikacji mWeryfikator nawiązywane jest połączenie Bluetooth i dokonywana jest weryfikacja czasu urządzeń, który nie może się różnić o więcej niż 5 (pięć) minut. W przypadku różnicy czasu większej niż 5 (pięć) minut lub w przypadku wygaśnięcia ważności Kodu QR przekazanie danych zakończy się niepowodzeniem;
 - d) Po nawiązaniu połączenia Aplikacja przekazuje do Aplikacji mWeryfikator dane Ucznia przekazującego dane, umożliwiając ich wyświetlenie w Aplikacji mWeryfikator oraz weryfikację poprawności jej Certyfikatu. Użytkownik Aplikacji mWeryfikator może dodatkowo zweryfikować przekazane dane online przy pomocy funkcji weryfikacji aktualności Certyfikatu;
 - e) Po prawidłowym zakończeniu elektronicznej weryfikacji danych osobowych Ucznia dane dotyczące dokonanej weryfikacji zapisywane są w Usłudze mLegitymacji (funkcja „Historia”).
- 3) Przy korzystaniu z powyższej funkcji „Przełącz” przekazywane są następujące dane:
 - a) numer legitymacji oraz data jej wydania,

- b) imię (imiona) i nazwisko Ucznia,
 - c) wiek Ucznia,
 - d) termin ważności mLegitymacji,
 - e) nazwa i adres szkoły,
 - f) zdjęcie o zredukowanej jakości.
- 4) Aplikacja mWeryfikator nie zapisuje danych Ucznia, którego dane zostały zweryfikowane z wykorzystaniem tej aplikacji. Wszystkie dane dotyczące tego Ucznia są usuwane z aplikacji mWeryfikator po wyjściu z ekranu wyświetlania danych.
 - 5) Wszystkie przypadki przekazania danych użytkownikowi Aplikacji mWeryfikator są zapisane w „Historii”. Funkcja „Historia” (dostępna z menu Aplikacji) pozwala na zapoznanie się z historią weryfikacji danych osobowych za pomocą Aplikacji mWeryfikator, zawierającą wyłącznie identyfikator użytkownika Aplikacji mWeryfikator oraz datę i czas przekazania danych.
 - 6) Funkcja „Historia” przechowuje dane, o których mowa w ustępie poprzedzającym, przez 1 rok od daty ich zapisania w Usłudze.

§ 6. Unieważnianie mLegitymacji i usuwanie danych Ucznia:

1. Funkcja usunięcia danych z Aplikacji (dostępna z menu Aplikacji) usuwa wszystkie dane przechowywane w Aplikacji oraz unieważnia Certyfikat. Po użyciu tej funkcji Aplikacja nie ulega odinstalowaniu z urządzenia mobilnego, jednak – aby mogła być ponownie używana – wymaga ponownego aktywowania, zgodnie z § 4 niniejszego załącznika.
2. Unieważnienie mLegitymacji jest dokonywane przez Dyrektora, następuje ono w przypadku:
 - 1) utraty ważności wydanej Uczniowi legitymacji szkolnej albo e-legitymacji szkolnej;
 - 2) utraty mLegitymacji na skutek uszkodzeń, niepoprawnego działania lub utraty urządzenia mobilnego, w którym przechowywana była mLegitymacji;
 - 3) w przypadku przejścia Ucznia do innej szkoły;
 - 4) na wniosek pełnoletniego Ucznia lub rodziców niepełnoletniego Ucznia.

§ 7. Prywatność i bezpieczeństwo

1. Podstawą przetwarzania danych osobowych w Aplikacji mLegitymacji przez Ministra Cyfryzacji jest art. 6 ust 1 lit. e Ogólnego rozporządzenie o ochronie danych w związku z art. 19f i 19h ustawy o informatyzacji.
2. Zgodnie z art. 19h ustawy o informatyzacji Minister przetwarza w systemie teleinformatycznym, o którym mowa w art. 19e, dane osobowe Uczniów w zakresie niezbędnym do obsługi dokumentów elektronicznych (mLegitymacji) oraz zapewnienia bezpieczeństwa teleinformatycznego i bezpieczeństwa obrotu prawnego.
3. Uczniowi przysługuje w dowolnym momencie prawo:
 - 1) dostępu do treści danych,
 - 2) ich poprawiania i sprostowania u Dyrektora,
 - 3) do usunięcia danych, np. za pomocą funkcji „usunięcia danych z Aplikacji”.

4. Uczniowi przysługuje również prawo do ograniczenia przetwarzania danych osobowych w przypadkach określonych w art. 18 Ogólnego rozporządzenia o ochronie danych. W takim przypadku Minister, na podstawie wniosku Ucznia, w systemie obsługującym mLegitymacje oznaczy dane i nie będzie ich poza ich posiadaniem przetwarzał, nawet w celach statystycznych do czasu wyjaśnienia sprawy.
5. Jeżeli Uczeń nie chce dalej korzystać z mLegitymacji, może poprosić Dyrektora o jej unieważnienie.
6. W przypadku zgubienia, kradzieży lub utraty z innych przyczyn urządzenia mobilnego, Uczeń powinien niezwłocznie dokonać zgłoszenia tego faktu Dyrektorowi.
7. Dla celu utworzenia Certyfikatu podczas aktywacji Usługi oraz zarządzania Certyfikatami Uczniów, w tym utrzymaniem listy aktywnych Certyfikatów, Minister przetwarza dane obejmujące imię, nazwisko, numer PESEL, numer legitymacji Ucznia.
8. Minister gromadzi dane statystyczne dotyczące Usługi w zakresie liczby:
 - 1) aktywacji mLegitymacji,
 - 2) akcji wydania Certyfikatów Ucznia,
 - 3) unieważnionych mLegitymacji,
 - 4) zgłoszonych problemów.
9. Z zastrzeżeniem ustępów następujących Minister nie przetwarza danych o połączeniach między urządzeniem mobilnym Ucznia używającego mLegitymacji a użytkownikiem Aplikacji mWeryfikator. Minister nie gromadzi również informacji o skorzystaniu przez Uczniów z funkcji elektronicznego przekazania danych lub elektronicznej weryfikacji danych osobowych.
10. Minister przy skorzystaniu z funkcji weryfikacji aktualności Certyfikatu Ucznia (sprawdzenie ważności Certyfikatu Ucznia online) za pomocą Aplikacji mWeryfikator gromadzi następujące dane:
 - 1) identyfikator użytkownika Aplikacji mWeryfikator,
 - 2) numer Certyfikatu Ucznia przekazującego dane, weryfikowanego za pomocą Aplikacji mWeryfikator.
11. Celem zbierania danych, o których mowa powyżej, jest sprawdzenie poprawności obsługi procesu weryfikacji aktualności Certyfikatu oraz wykrycia ewentualnych błędów i luk bezpieczeństwa.
12. Dane, o których mowa w tym ustępie przechowywane są przez okres 6 lat od dnia ostatniej aktywności Użytkownika w systemie teleinformatycznym Aplikacji (art. 19h ustawy o informatyzacji). Dane nie są przetwarzane w celach marketingowych.
13. Administratorem danych zawartych w mLegitymacji jest Dyrektor, do której uczęszcza Uczeń.
14. Administratorem danych osobowych Użytkownika zawartych w Certyfikacie Ucznia jest Minister, mający swą siedzibę w Kancelarii Prezesa Rady Ministrów, al. Ujazdowskie 1/3, 00-583 Warszawa. Z administratorem można się kontaktować na podany wyżej adres lub na adres ul. Królewska 27, 00-060 Warszawa lub elektronicznie, na adres: Kancelaria.Krolewska@mc.gov.pl lub na adres skrytki ePUAP: /MAiC/Skrytka-

ESP. Administrator wyznaczył Inspektora Ochrony Danych, z którym można się kontaktować w sprawach związanych z przetwarzaniem danych osobowych przez Ministra bezpośrednio pod adresem: iod@mc.gov.pl.

15. Dane nie są przetwarzane w celach marketingowych.
16. Dane osobowe Ucznia będą mogły również być przetwarzane przez podmioty przetwarzające w imieniu administratora (Ministra), to jest przez:
 - 1) Centralny Ośrodek Informatyki, Aleje Jerozolimskie 132-136, 02-305 Warszawa,
 - 2) Naukową i Akademicką Sieć Komputerową - Państwowy Instytut Badawczy, ul. Kolska 12, 01-045 Warszawa.
17. Dane osobowe mogą być przekazywane do organów publicznych i urzędów państwowych lub innych podmiotów upoważnionych na podstawie przepisów prawa lub wykonujących zadania realizowane w interesie publicznym lub w ramach sprawowania władzy publicznej.
18. Dane osobowe Ucznia nie będą podlegały zautomatyzowanemu podejmowaniu decyzji, w tym profilowaniu.